REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Rejection of Claims 1-4, 13-25, and 34-41 Under 35 USC §102(e) in view of U.S. Patent No. 6,061,449 (Candelore)

This rejection is again respectfully traversed on the grounds that the Dunlavy patent, like the Candelore patent fails to disclose or suggest execution of commands in the operating program of a data carrier in such a way that the data processed by the corresponding commands cannot be inferred from signals detectable from outside the semiconductor chip of the data carrier, as recited in independent claims 1, 22, and 34. To the contrary, the Dunlavy patent actually *teaches away* from the claimed invention.

As indicated in the previous response, the Candelore patent discloses a procedure for "scrambling" encrypted program information and authentication information being communicated from an external storage device to the buffers of a secure circuit, so that the programming sequence of the secure circuit cannot be detected by intercepting the communicated data, by **changing the sequence in which a secure circuit retrieves data from the external storage device** in order to hide the order of execution of the program steps. Thus, the Candelore patent differs from the claimed invention in the following manner:

Candelore: teaches changing sequence of data retrieval from external memory

Claimed: modify execution of commands by a data carrier to prevent commands from being inferred by signals radiated by the data carrier

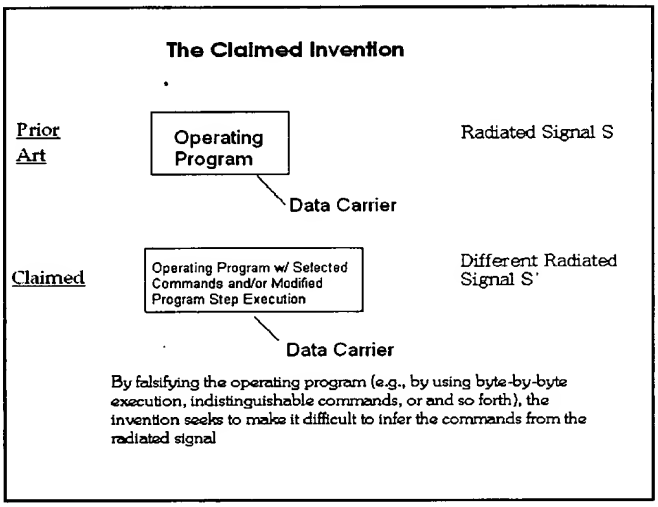
Therefore, in order for the rejection to be proper, the Dunlavy patent must suggest modification of the communication-protection scheme of Candelore to protect commands being executed on a chip, as opposed to scrambling communications. However, instead of suggesting modification of Candelore's communication protocol to affect program execution, the Dunlavy patent actually ***teaches away*** from the claimed modification.

The signal detection prevention method of Dunlavy differs from the claimed invention in at least the following respects:

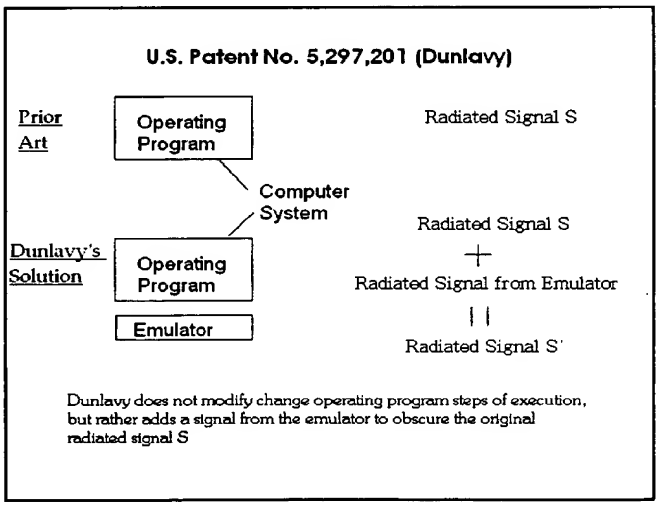
a. Dunlavy concerns protection of data in a computer system, rather than protection of program execution in a data carrier of the type claimed;

b. **Dunlavy does not attempt to modify execution of programs in the computer system being protected, but rather lets the programs execute normally, and at the same time sends out false signal emissions that mask the original signal emissions.**

Applied to the Candelore system, the teaches of Dunlavy would at best involve generation of false communication signals to mask the scrambled data communications taught therein. This is not the same as modifying program execution by a data carrier (*or a computer system*), as claimed.



Basically, as indicated in the Figures included herewith, Dunlavy approaches the problem of radiated signal detection by adding a masking signal to the radiated signal. Dunlavy is not concerned with execution of the program that causes the radiated signals, but with the signals themselves.



The claimed invention, on the other hand, approaches the problem by addressing the underlying operating program. The claimed approach is much more practical for a data carrier, since it would be difficult to add

an emulator to a data carrier of the type claimed (as opposed to an entire computer system of the type with which Dunlavy is concerned). **In other words, instead of altering data and commands so that signals or commands are difficult to detect from radiated signals, Dunlavy suggests provision of a separate emulation circuit to merely emulate the non-altered data and commands of the executing computer in order to mask the signals radiated during execution of the non-altered data and commands.**

Since the Dunlavy patent does not disclose or suggest the basic command hiding approach recited in the independent claims, it could not possibly have suggested modification of the Candelore communication scrambling method to include the specific falsification methods recited in the dependent claims, such as:

a. execution of the commands using byte-by-byte processing of data (as opposed to bit-by-bit processing), as recited in **claims 2 and 23**;

b. choosing commands that generate indistinguishable signal patterns, as recited in claims **3 and 24**,

c. choosing commands that lead to signal patterns which are substantially independent of the data processed, as recited in **claims 4 and 25**; or

d. changing the order of execution of operations, as recited in claims **13-19 and 34-40**.

Instead, Dunlavy discloses emulation signal generation, while the Candelore patent concerns a procedure for "scrambling" encrypted program information and authentication information being communicated from an external storage device to the buffers of a secure circuit, so that the programming sequence of the secure circuit cannot be detected by intercepting the communicated data. Neither approach involves protecting data input operated upon by the operating program of a data carrier semiconductor chip through detection of signals radiated by the chip. Instead, Candelore (in effect) simply hides the order of execution of program steps by the secure circuit by changing the sequence in which the secure circuit retrieves data from the memory, while Dunlavy adds a parallel emulation generator to generate additional radiation signals that will mask the original signals.

Dunlavy concerns a problem that is similar to that of the claimed invention, namely inferring data or programs from radiated signals, but adopts an alternative solution that does not correspond to the claimed invention, and therefore the Dunlavy patent could not have suggested modification of the Candelore system to obtain the claimed invention. Withdrawal of the rejection of claims 1-4, 13-25, and 34-43 under 35 USC §103(a) is accordingly respectfully requested.

5. Rejection of Claims 5-12 and 26-33 Under 35 USC §102(e) in view of the Candelore and Dunlavy Patents, and U.S. Patent No. 6,373,946 (Johnston)

This rejection is respectfully traversed on the grounds that the Johnston patent, like the Candelore and Dunlavy patents, does not disclose or suggest execution of commands in the operating program of a data carrier in such a way that the data processed by the corresponding commands cannot be inferred from signals detectable from outside the semiconductor chip of the data carrier. Instead, the Johnston patent merely relates to encryption of data by a semiconductor chip. There is nothing in the encryption method of Johnston to prevent an attacker from analyzing signals emitted by the chip that does the encryption in order to deduce the program steps used in the encryption and thereby reconstruct the encryption keys based on the deduced program steps and an intercepted output.

As explained in the previous response, the Johnston patent concerns a particular encryption method for securing communications, involving use of a common encryption key, transmittal of the key is a secure memory using the exclusive OR operation to mask the keys. While masking of the keys using the XOR operation is a technique that is also used by the present invention (and in fact is a very basic data masking technique), the key masking is not used in the same way as that of the claimed invention. In Johnston, the keys are masked using exclusive OR, *and then* ***unmasked*** *at the receiving end so that they can be used to decrypt the transmitted communication.* **There is no modification of the decryption algorithm to compensate for the masked keys.** In the claimed invention, the masked input data is directly applied to the processing operations carried out by the chip, and the processing operations are varied accordingly so that the **processor**

performs modified operations on modified input data. As a result, only the modified input data can be inferred from the signals emitted by the chip during processing.

Because the Johnston patent is not at all concerned with signals emitted by the chip during execution of program steps, but only with the overall results of the execution, *i.e.*, with communications between processors, it is respectfully submitted that the Johnston, Candelore, and Dunlavy patents could not have suggested the claimed modification of program step execution to make it more difficult to infer program step execution by statistical analysis of radiated signals, and therefore withdrawal of the rejection of claims 5-12, and 26-33 under 35 USC §103(a) is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: May 20, 2005

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500